eMPN Security Corrective Action Plan
Task Order 65 - Deliverable 65.1.3
E-Sign Mad Dog

SFA needs to address several security issues that remain outstanding for the eMPN. The matrix below documents several items that have either been identified previously but remain outstanding, or new issues that have not yet been documented. Attached to this document is an appendix to the IATO letter completed by EDS for the eMPN certification effort at the June 28, 2001 Production Readiness Review. The appendix outlines areas needing corrective action which were identified in past security assessments. Although the corrective action items in the appendix addresses Loan Origination Subsystem (LOS) security as a whole, specific attention should be given to how the items may affect the security of the eMPN DLO and ePN DLC websites, once the websites are on-line and fully operational.

To understand the totality of security controls and respond to this corrective action plan, it will be necessary to obtain security information from the contractors responsible for other components of the LOS system, CSC and NCS. Specifically, information regarding operating system security and the network and physical security of the e-promissory note web servers in question will be required.

eMPN Security Corrective Action Plan

No.	Observation	Concur with Observation	Corrective Action / Description	Completion Date	Point of Contact
1	Finding: Security management for eMPN is divided among three contractors: EDS, NCS Pearson, and CSC. Clear areas of security responsibility have not been identified. The eMPN Web Server falls under the same direct hardware, network and operating system control as the LO/LC Web servers, which are administered by CSC. The eMPN websites share common functionality with the LO/LC Websites as they provide the end user with information pertaining to the user's Loan Origination and Loan Consolidation information, and add the option for the end user to electronically sign her or his P-Note. Recommendation: SFA should encourage each party responsible for any portion of the eMPN to mutually draft written areas of security responsibility. There may be considerable difficulty in correcting this issue due to the inherent complexity when addressing application vs. infrastructure security.				
2	Finding: There is no trading partner agreement among the eMPN contractors. Recommendation: A trading partner agreement should be established among the eMPN contractors to include performance level agreements, service level agreements, security responsibility, etc.				

No.	Observation	Concur with Observation	Corrective Action / Description	Completion Date	Point of Contact
3	Finding: Currently, no addenda has been written for the CSC Security Plan for the LO and LC websites or the VDC to include all application and infrastructure level controls associated with eMPN. Recommendation: EDS has stated they will draft the addenda for the LO and LC websites. The addenda should be coordinated with CSC's effort to update the infrastructure portion of the VDC security plan.				
4	Finding: The security controls identified in section 3.1 of the IATO document are not all verified or validated. Recommendation: CSC and NCS Pearson should verify and validate their respective security controls as identified in section 3.1 of the IATO document. EDS has performed this task for the security controls in their area of eMPN responsibility.				
5	Finding: The IATO contains an application layer view of the eMPN, but there is no hardware and network architecture view. Recommendation: CSC, as the contractor responsible for the hardware and network supporting the eMPN, should develop a hardware and network architecture graphic.				